REMARKS/ARGUMENTS

Applicant respectfully requests reconsideration and allowance of the subject application.

Claims 1-21 were originally submitted.

Claims 11-21 are withdrawn without prejudice per a Restriction Requirement of an earlier communication.

No claims are amended in this response.

No new claims are added.

Claims 1-10 remain in this application.

35 U.S.C. §102

Claims 1, 4, 5 and 8 have been rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,141,423 to Fischer (Fischer). Applicant respectfully traverses the rejection.

In order to prevent the transfer of any escrowed information within a computer to some body other than a legitimate owner, Fischer teaches a method that employs a voluntary identification/definition performed after a computer is purchased, and a secret information retrieval phase. The escrowed information is any information stored on a computer which has been encrypted through a third party encryption. See Fischer, col. 1, lines 42-52.

In particular, the mechanisms taught by Fischer include third party authentication and verification for determining the ownership of the escrowed information. In the definition phase, the true owner/customer defines an escrow record that provides self identification data together with encrypted password or any other secret data. The identification indicia is combined with the secret

information (e.g., the user's encryption password) and is encrypted under the control of a trustee's public key. As the user enters the unique identification data, he is asked to select a password to protect the system. Thereafter, all the personal identifying data together with the password is encrypted with the manufacturer's (trustee's) public key and is stored in the user's computer as an escrow security record. The secret information retrieval phase of the invention is of use in cases when the user forgets his/her password. See Fischer, col.2, lines 41-67; col.10, lines 14-53; Fig.6; Col. 12, lines 13-18.

Fig. 6 of Fishers shows a flowchart of a sequence of operations performed when an applicant attempts to retrieve escrowed secret information. The applicant may either be a legitimate owner of the information or a person attempting to steal valuable information. The applicant initially provides the trustee with the escrow information record which has been encrypted with the trustee's public key. The applicant further presents the trustee with the documentation containing credentials that can be matched with the escrowed information. The request for the secret information must be verifiable with the same public key that is in the escrow record. Moreover, the physical appearance of the applicant must match the described characteristics in the standard identifying information. The trustee performs a matching of the hash value of the escrow record with the hash value supplied to him by the applicant. If these values match, the trustee is assured that the escrow record has been delivered in the correct form. Based on these criteria, the trustee determines whether the applicant is a legitimate owner or someone who has a genuine claim to the data.

If the applicant turns out to be a legitimate owner, the secret information is provided to him and he decrypts the supplied secret escrowed information using the appropriate private key.

Independent claim 1, recites "[a] computer-implemented method comprising:

> sending a request for network account credentials from an originating account associated with an unpublished object at a dispatch associated with a published object, the request directed to the published object associated with the dispatch includes identification of the unpublished object associated with the originating account;
>
> authenticating the originating account at the dispatch; and,
>
> upon authenticating the originating account, sending an emblem that includes an object and credential, for a network account to the originating account, the emblem sent to the unpublished object associated with the originating account and having the identification as included with the request.

Fischer does not disclose "upon authenticating the originating account, sending an emblem that includes an object and credential for a network account to the originating account, the emblem sent to the unpublished object associated with the originating account and having the identification as included with the request." as recited in claim 1.

As discussed above, Fischer discloses a transfer of decrypted escrow information along with secret credentials once authentication is successful. The transferred escrow information includes only decrypted information and is used

essentially by a trustee in the process of identifying whether an applicant of secret information is the legitimate user.

Fischer discloses that during authentication of an applicant, some information is required about the applicant. Preferably this information is stored on the applicant's computer in an encrypted manner. This information is referred to as an escrow record and further includes a field that secretly holds a key which can decrypt entire data stored on the applicant's computer. Whenever an applicant requires secret credentials to decrypt entire data on his computer he sends the encrypted escrow record to the trustee. The trustee in turn decrypts the escrowed record to establish that the applicant is the legitimate owner of the information and to retrieve the secret key stored on the escrow record. Once the determination is done the trustee sends the secret credentials along with the decrypted escrow record to the applicant. See Fischer, col.8, lines 6-35; col.10, lines 14-55; col. 12, lines 12-18.

In contrast, the application describes a transfer of an emblem which contains a secret credential and an object. The object is capable of storing data and instructions, it can include files, message queues etc. For example, see specification page 13 line 21 to page 14 line 3. The object generally stores instructions assigned by a dispatch which are to be done to accomplish batch processing. It is further disclosed that the emblem can be used to store and transfer both instructions for batch processing and credentials to access information required to carry out the instructions. There is no mention of such a transfer of an emblem in Fischer stores and transfers both credentials and object.

Correspondingly, Fischer does not disclose "upon authenticating the originating account, sending an emblem that includes an object and credential for a

network account to the originating account, the emblem sent to the unpublished object associated with the originating account and having the identification as included with the request" as recited in claim 1. We therefore believe that successful arguments can be made on these bases to overcome the Office's rejection of independent claim 1.

Accordingly, Fischer does not show every element of claim 1, and the rejection of claim 1 is therefore improper. Accordingly, Applicant respectfully request that the §102 rejection of claim 1 be withdrawn.

Dependent claims 4, 5 and 8 depend from claim 1, and are allowable at the least for reasons provided in support of claim 1. Accordingly, Applicant respectfully request that the §102 rejection of claims 4, 5 and 8 be withdrawn.

Claim 8 further recites "wherein the network account for which the emblem is sent from the dispatch to the originating account comprises an agent account of an agent".

Fischer teaches transferring a secret decryption key to a user once it is determined that the user is the legitimate owner of the escrowed information. There is no mention of sending an emblem from the central authority (dispatch) to the originating account (requesting user) includes an agent account of an agent. Fischer teaches a transfer of a secret decryption key to field a request from a user. Furthermore, the request is made by the user to retrieve the coded escrowed information which can be decrypted only by the secret key residing with a third party (escrow trustee). Additionally, the communication is directly between the trustee and the user requesting the decryption key. The mechanism suggested by Fischer is just a validation and authentication procedure to ensure that the

requesting user is a legitimate owner of the escrowed information. See Fischer, col. 11, lines 4-16; col. 12, lines 12-18.

The Application discloses a mechanism where an emblem is sent from the central authority (dispatch) to the requesting user (originating account) through an agent account of an agent. For example, see Application, page 11, lines 10-22; page 12 line 20 through page 13 line 5. The central authority uses an agent account in a situation that requires grant of global access privileges to more than one client computer on a distributed network. During batch processing over a distributed network it may be required that global access rights, normally assigned to only network accounts like that of a central authority (dispatch) should be given to client computers involved on batch processing. The central authority may be allowed to simultaneously grant global access rights to more than one originating accounts. In particular, the central authority transfers it's rights to the originating accounts through proxy logging onto the agent accounts and then remoting to the originating accounts. In comparison, Fischer fails to teach or disclose fielding requests of originating accounts by transfer of emblems through agent accounts.

35 U.S.C. §103

Claims 2, 3 and 4 have been rejected under 35 U.S.C. 103(a) as being unpatentable by Fischer. Applicant respectfully traverses the rejection.

Claims 2, 3 and 4 depend on claim 1 and are allowable based on arguments presented above in support of claim 1. Accordingly, Applicant respectfully request that the §103 rejection of claims 2, 3 and 4 be withdrawn.

Claims 6 and 7 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to independent claim 1 and further in view of

US patent No. 5,613,012 issued to Hoffman et al. (Hoffman). Applicant respectfully traverses the rejection.

Claims 6 and 7 depend on claim 1 and are allowable based on arguments presented above in support of claim 1. Accordingly, Applicant respectfully request that the §103 rejection of claims 6 and 7 be withdrawn.

Claim 9 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to claim 1 and further in view of US patent No. 5974566 issued to Ault et al. (Ault). Applicant respectfully traverses the rejection.

Claim 9 depends on claim 1 and is allowable based on arguments presented above in support of claim 1. Accordingly, Applicant respectfully request that the §103 rejection of claim 9 be withdrawn.

Claim 10 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to claim 1 and further in view of US patent No. 6,006,018 issued to Burnett et al. (Burnett). Applicant respectfully traverses the rejection.

Claim 10 depends on claim 1 and is allowable based at least on arguments presented above in support of claim 1.

Claim 10 further recites "wherein the emblem is expirable, such that the method further comprises determining whether the emblem is about to expire, and upon so determining, renewing the emblem with a renewing authority."

Burnett fails to teach or suggest this element. Burnett teaches a mechanism to restore mapping upon expiration of an authentication period of mapping between different file systems. In general, Burnett teaches a mechanism to facilitate interoperability and coexistence of different distributed file systems within a distributed computing environment (DCE) domain. This is achieved by mapping credentials associated with a requesting user into credentials containing

authentication information associated with a target distributed file system's authentication model or paradigm. Subsequently, a connection is established between the requesting user and the target file system through a VFS (virtual file system) switch. Burnett further teaches that a user in a DCE can determine when his/her credentials will expire using a Klist command; however, Burnett admits this determination cannot be done in a NFS/DFS translator model because there is not a running process on the translator system which DCE credentials can be associated with to perform the Klist command. Therefore, a translator user cannot list his credential information. Furthermore, Burnett admits that the user is not notified when his/her mapping has expired. Moreover, when DCE credentials expire a translator user is not able to renew his credentials. See Burnett, col.22, lines 19-46; col.1, lines 48-67; col.2, lines 1-17 ; col.2, lines 53-67).

The application describes a mechanism in which the emblems are expirable, such that they are only valid for a limited period of time, to add another level of security within the system. When the emblem is about to expire, it is renewed with a renewing authority so that the originator that is the holder of the emblem can continue to access system resources as allowed by the network access credentials encased within the emblem. See for example, Application, page 17, lines 20-23 through page 18 lines 1-3; page 14, lines 20-23 ; page 15, lines 1-4. Burnett teaches a mechanism to determine credential mapping status.

CONCLUSION

All pending claims 1-10 are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the subject application. If any issues remain that prevent issuance of this application, the Examiner or Office is urged to contact the undersigned attorney before issuing a subsequent Action or Communication.

Respectfully Submitted,

Dated: October 31, 2007

By: /Emmanuel A. Rivera/
Emmanuel A. Rivera
Reg. No. 45,760
(509) 324-9256 ext. 245